

DOGE's .gov site lampooned as coders quickly realize it can be edited by anyone

"An official website of the United States government," reads small text atop the Department of Government Efficiency (DOGE) website that Elon Musk's team started populating this week with information on agency cuts.

But you apparently don't have to work in government to push updates to the site. A couple of prankster web developers told 404 Media that they separately discovered how "insecure" the DOGE site was, seemingly pulling from a "database that can be edited by anyone."

One coder couldn't resist and pushed two updates that, as of this writing, remained on the DOGE site. "This is a joke of a .gov site," one read. "THESE 'EXPERTS' LEFT THEIR DATABASE OPEN," read another.

404 Media spoke to two other developers who suggested that the DOGE site is not running on government servers. Instead, it seems to be running on a Cloudflare Pages site and is relying on a database that "can be and has been written to by third parties and will show up on the live website," the developers told 404 Media.

Archived versions of the DOGE site show that it was basically blank before Tuesday. That's when Musk held a DOGE press conference in the Oval Office, promising that DOGE is "actually trying to be as transparent as possible." At that time, Musk claimed that DOGE was being "maximally transparent" by posting about "all" actions to X (Musk's social media

platform) and to the DOGE website. (Wired deemed the DOGE site “one big X ad” because it primarily seems to exist to point to Musk’s social media platform.)

According to 404 Media, after Musk made that statement, his team rushed to build out the DOGE website, mirroring X posts from the DOGE account and compiling stats on the federal workforce.

But in rushing, DOGE appears to have skipped security steps that are expected of government websites. That pattern is troubling some federal workers, as DOGE has already been dinged by workers concerned by Musk’s team seizing access to sensitive government information and sharing it in ways deemed less secure. For example, last week, Department of Education officials raised alarms about DOGE employees using personal emails viewed as less secure than government email addresses, seemingly in violation of security protocols. These personal emails also seemed to shroud the true identities of DOGE staffers, whereas other government employees must use their full names in official communications.

<https://arstechnica.com/tech-policy/2025/02/doges-gov-site-lam-poored-as-coders-quickly-realize-it-can-be-edited-by-anyone/>